CUSTOMER OWNED BANKING
CODE COMPLIANCE COMMITTEE

Privacy
Own Motion Inquiry

A review of customer owned banking institutions' compliance with privacy obligations under Section D23 and Key Promise 8 of the Customer Owned Banking Code of Practice

June 2018

The Code

The Customer Owned Banking Code of Practice (the Code) was developed by the Customer Owned Banking Association (COBA) and commenced operation on 1 January 2014. The Code replaces the 2010 Mutual Banking Code of Practice.

The Code has been revised to accommodate changes the Australian Securities and Investments Commission (ASIC) made to Regulatory Guide 221 *Facilitating digital financial services disclosures* and the *e-Payments Code*. The revised Code has been effective from 1 July 2016.

Through the Code, 67 subscribing[1] credit unions, mutual banks and mutual building societies voluntarily commit to fair and responsible customer owned banking. The Code contains ten key promises stating that these institutions will:

- be fair and ethical in dealings with customers (including small businesses)
- focus on customers in their service delivery
- give customers clear information about products and services
- be responsible lenders
- deliver high customer service and standards
- deal fairly with any complaints
- recognise their customers' rights as owners of the institution
- comply with legal and industry obligations
- recognise their impact on the wider community, and
- support and promote the Code of Practice.

The Committee

The Code Compliance Committee (the Committee) is an independent compliance monitoring body established under the Code and the Code Compliance Committee Charter (the Charter). It comprises an independent chair, a person representing the interests of the customer owned banking sector and a person representing the interests of consumers and communities. The Code and Charter entrust the Committee with several functions and responsibilities, including to:

- conduct 'Own Motion' inquiries into compliance with aspects of the Code, and
- provide advice to COBA on training and other activities necessary to assist subscribers to meet their Code requirements.

Definitions

For ease of reference when reading this report:

- 'the Code' means the 2016 Code unless otherwise stated
- 'consumer/customer' includes individuals or small businesses that are members or customers of Code subscribers, and
- 'institution' means a customer owned banking institution that subscribes to the Code.

[1] Number of Code subscribers as at June 2017.

Contents

Executive Summary

Customer owned banking institutions hold a wealth of customer data and have explicit legal, regulatory and self-regulatory obligations to collect, manage and use this personal information appropriately. These obligations, primarily set out in the *Privacy Act 1988* (Cwlth) (Privacy Act) and Australian Privacy Principles (APPs), are reiterated and extended in the Customer Owned Banking Code of Practice (the Code). As Australia moves towards implementing open banking, privacy and data security compliance will become both increasingly complex to manage and more vitally important.

In this context, institutions' high level of non-compliance with existing privacy obligations in the Code is cause for concern. To consider and address these privacy issues, the Code Compliance Committee (the Committee) launched an Own Motion Inquiry into institutions' compliance with the privacy obligations in Section D23 and Key Promise 8 of the Code. To do this, the Committee gathered information from 67 Code-subscribing institutions with an online questionnaire (at **Appendix 1**).

Collecting personal information

Institutions can collect information that is reasonably necessary but are bound by APPs setting out how this is to be done. All 67 Code subscribing institutions have mechanisms in place to prevent the collection of unnecessary personal information, to handle unsolicited information and to obtain consent before collecting sensitive information.

Managing personal information

Under the APPs and the Code, institutions are bound by a range of requirements concerning how personal information is managed. All institutions described reasonable steps they take to control staff access to personal information and protect it from theft, unauthorised access, disclosure or loss. Institutions also have appropriate procedures for making corrections to personal information and destroying or de-identifying it when it is no longer needed.

Using personal information

Managing how personal information is used, already a complex area of compliance, will increase in complexity and importance with the introduction of open banking. Here, the inquiry found room for institutions to embrace a higher standard of practice, giving customers more control of how their data is used by making it easier to opt-out of direct marketing and by ensuring that customers understand and meaningfully consent to any disclosure of their information to third parties.

Managing compliance with privacy obligations

To achieve and maintain compliance with the Privacy Act and the Code, institutions must have an appropriate privacy policy in place; train staff in their privacy obligations; and regularly review the privacy compliance framework in the organisation.

All institutions reported that they have a comprehensive privacy policy that is accessible to customers. Although all institutions also have training processes in place, the frequency of breaches caused by human processing error indicates that institutions need to do more to keep privacy requirements front-of-mind for staff. Most institutions review their privacy compliance at least once every two years, although it appears that these reviews could be more comprehensive.

Recommendations

Open banking and the future of privacy

1. In the open banking environment, institutions' data storage and transfer processes and procedures should be updated to address the increased risk of hacking and unauthorised access.

2. Institutions should proactively monitor their compliance with privacy obligations, rather than relying exclusively on customer complaints to identify issues.

Collecting personal information

3. Institutions should prevent the collection of unnecessary or irrelevant information.
4. Institutions should have appropriate processes for seeking consent, preferably written consent for the collection of sensitive information.
5. Institutions need processes and procedures for destroying unsolicited and unnecessary information.

Managing personal information

6. Institutions should ensure that password protocols are strong, and that staff never share passwords.
7. Institutions should have a clean desk policy.
8. Institutions should ideally have banking system restrictions in place.
9. Institutions should have robust processes and procedures for verifying the identity of persons requesting access to personal information.
10. Institutions should review the adequacy of their security arrangements at least annually.
11. New processes and technologies should prompt privacy impact and risk assessments before any third-party contractors are engaged.

12. Institutions should systematically review their privacy and security settings. This should include – but not be limited to – testing security settings.
13. Manual reviews and spot checks should be supplemented by regular system-wide reviews of data accuracy. Where appropriate, they should use information from third parties and other sources to update customer information.
14. Institutions should take reasonable steps to confirm and correct information, including contacting customers. They should check that inaccurate, out-of-date, incomplete, irrelevant or misleading information has not impacted the customer or third parties before removing it from the system.
15. Institutions should have a policy and processes for destroying or de-identifying unneeded information, including digital information.

Using personal information

16. Institutions should ensure their privacy procedures cover how information can be used for direct marketing and when it can be disclosed to other parties, as well as how customers can access their own data.
17. Institutions should follow good practice by making direct marketing an opt-in choice. At a minimum, they must have clear, plain English avenues for opting out.
18. Institutions should specifically develop privacy consents to support understanding, using concise, plain English expression and user-friendly design.
19. Institutions should review their privacy consent processes considering open banking requirements.
20. Institutions should develop processes for providing written refusal of a customer's request for access to information.
21. Institutions should review their compliance with privacy requirements on information disclosure to guarantors. They should only provide information concerning the loan, including the current balance of the debtor's account; any amounts credited or debited during a period specified in the request; any amounts currently overdue and the dates they became due; and any amount currently payable and the date it becomes due. They must not provide information about a customer's transaction or savings accounts.

Managing compliance with privacy obligations

22. Institutions should provide ongoing and refresher training, as well as routine staff alerts and reminders of privacy obligations to all staff that have contact with customer personal information.
23. Institutions should conduct a comprehensive privacy review annually.

24. Institutions should ensure that there are strict contractual Service Level Agreements (SLAs) in place with all third-party suppliers that have access to customer information and that these are regularly monitored of performance against the agreed SLAs. Examples of third parties include customer statement printers, IT software providers, external help desks, auditors, etc.
25. Institutions should review how they deal with overseas disclosure.
26. Institutions should ensure that their privacy policies are visible and readily accessible to customers.

For a privacy compliance checklist see page 30.

Introduction

Privacy and data security is a crucial area of compliance for customer owned banking institutions, and the importance and complexity of these obligations is only increasing. As the Australian Privacy Commissioner, Timothy Pilgrim, noted in relation to the recent commencement of the Notifiable Data Breaches scheme, the success of organisations that handle personal information now depends on trust: 'people have to trust that their privacy is protected, and be confident that personal information will be handled in line with their expectations.'[2]

In this context and given the relatively high level of non-compliance with existing privacy obligations, the Customer Owned Banking Code Compliance Committee (the Committee) determined that it was important to conduct an in-depth investigation into institutions' privacy compliance.

This report describes the findings of the Committee's inquiry into how Australia's customer owned banking institutions protect their customers' privacy, and the level of compliance with their obligations under privacy legislation and related requirements in the Customer Owned Banking Code of Practice (the Code).

Methodology

This inquiry was based on information provided by Code subscribers and the Committee's analysis of that information. Information was gathered via individual telephone conferences and an online questionnaire. To gather information and examples of good practice regarding compliance with Code obligations and the APPs, an online questionnaire (at Appendix 1) was sent to all Code subscribers in November 2017. Participating institutions by size, measured by assets and number of active members, are shown in **Table 1**.

Table 1: Participating institutions in online questionnaire

	Size of institution (measured by number of active members)					
Size of institution measured by $amount in assets	**Up to 10,000**	**Between 10,000 and 50,000**	**Between 50,000 and 100,000**	**Between 100,000 and 200,00**	**Over 200,000**	***TOTAL***
Micro (<$200m)	20	7	-	-	-	***27***
Small ($200m to $500m)	4	6	-	-	-	***10***
Medium ($500m to $1b)	-	10	-	-	-	***10***
Large (>$1b)	-	5	7	3	5	***20***
TOTAL	***24***	***28***	***7***	***3***	***5***	***67***

[2] Pilgrim, Timothy (2018) 'Commencement of the notifiable data breaches scheme', keynote address at the Optus Information Security, Sydney, 22 February. Available at https://oaic.gov.au/media-and-speeches/speeches/commencement-of-the-notifiable-data-breaches-scheme.

Complementing data from the questionnaire, individual telephone conferences were held with all 17 institutions above $1b in assets (large) and seven other institutions (three micro, one small and three medium institutions) that self-reported a high number of privacy Code breaches and complaints in the 2017 Annual Compliance Statement (ACS). The telephone conferences were undertaken as part of the annual ACS Verification Program to obtain more detailed and specific information about privacy breaches, training, procedures, processes and reporting.

Privacy and the customer owned banking sector

While providing their services, customer owned banking institutions necessarily collect and hold a great deal of customer data. This spans customers' demographic information, such as where they live and work; detailed financial information about their assets, income and expenses; and information about their lifestyles, namely how they spend their money. Less commonly, institutions also have reason to collect sensitive information, such as information about a customer's health conditions and professional and trade organisation memberships.

Institutions' privacy obligations

Australian law recognises that people have the right to make choices and have some control over how such information about them is used and shared.[3] Privacy rights can afford protection from serious detriment, like identity fraud, theft,[4] and exposure to family violence; and from intrusion, such as unwanted marketing. Therefore, customer owned banking institutions, like other financial services providers, have strong legal, prudential and regulatory obligations to manage data and security risks.

Primary among these obligations is compliance with Australia's key privacy legislation, the *Privacy Act 1988* (Cwlth) (Privacy Act). The Privacy Act regulates how entities handle an individual's personal information – that is, any information about an individual whose identity is apparent or can reasonably be ascertained.[5] The Privacy Act includes thirteen APPs.[6] The APPs set out standards, rights and obligations relating to how personal and sensitive information can be collected, handled, held, used, accessed and corrected.

---

[3] Pilgrim, Timothy (2014) 'Privacy matters', public lecture at Griffith University, Brisbane, 8 May. Available at https://www.oaic.gov.au/media-and-speeches/speeches/privacy-matters

[4] *Ibid.*

[5] It includes an opinion or evaluative material. Even if the information is not true, it is protected if it relates to an identifiable individual.

[6] See Appendix 2.

The Code reiterates and extends institutions' Privacy Act obligations. Key Promise 8[7] of the Code is a general requirement that institutions comply with legal and industry obligations, among which are the Privacy Act obligations. The Code also contains Section D23,[8] which sets out specific requirements concerning:

- compliance with privacy laws
- use and disclosure of information
- protection of information
- access to information
- the institution's own privacy policy, and
- retention of privacy information.

These Section D23 obligations are consistent with obligations under the Privacy Act and the general law duty of confidentiality.

The Customer Owned Banking Association (COBA) has developed additional guidance, *Customer Owned Banking Code of Practice Compliance Manual,* to support institutions to comply with these legal and Code obligations.[9] COBA has also issued an *Australian Privacy Principles Compliance Manual* and *Record Retention – a Guide to your Legal Obligations*, as well as templates and training modules to assist institutions to comply.

Open banking and the future of privacy and data security

Managing privacy and data security will soon become increasingly important and complex as technological innovation, regulatory change and shifting customer preferences profoundly transform the financial services sector.

The major development is the introduction of 'open banking'. At present, individual institutions retain and control whatever customer information they gather. Open banking, conversely, will place customers in control of their data, enabling them to share it with the approved third parties they choose. Open banking is expected to drive competition and the evolution of new products and services.

For example, customers may be able to use new budgeting apps by sharing information about their spending habits and regular payments. Similarly, by providing their data to switching services, customers may be able to get more customised and accurate recommendations for different financial products and services.

---

[7] See Appendix 3.

[8] See Appendix 3.

[9] See Customer Owned Banking Code of Practice Compliance Manual, p. 105–110.

In Australia, implementation of open banking is in its early stages. Comprehensive Credit Reporting, a component of open banking, has already been mandated and will begin taking effect from 1 July 2018. In December 2017, the Australian Government Treasury's Review into Open Banking in Australia (the Farrell Review) set out recommendations for the open banking regulatory framework and operating model.

The big four banks have signed up for open banking, and while COBA has recommended that open banking should initially be voluntary for its member institutions, it anticipates that a number will be early adopters.[10]

Open banking is expected to amplify privacy and security risks and make privacy management more complex. Although some existing privacy risks will be reduced, more points of data storage and data transfer will increase risks of hacking and unauthorised access.[11] Ensuring that customers understand what they are agreeing to when they share their data will become more complex, as will the processes of recording and managing customer consents, permissions and data connection requests.[12]

In the open banking environment, institutions' data storage and transfer processes and procedures should be updated to address the increased risk of hacking and unauthorised access.

Implementing open banking will entail changes to the Privacy Act as well as the introduction of new legislative and regulatory rules, so institutions will need to be prepared to adapt to shifting obligations.

Compliance with privacy obligations

In recent years, the customer owned banking industry has seen high levels of non-compliance with privacy obligations. Non-compliance with privacy obligations is currently a major source of self-reported breaches of the Code.

In the 2017 Annual Compliance Statement (ACS), 24% of self-reported Code breaches related to privacy and confidentiality issues (Section D23). Privacy non-compliance was similarly high the previous year, accounting for 30% of self-reported Code breaches, including five significant Code breaches (**Table 2**).

---

[10] Customer Owned Banking Association, 29 September 2017, Submission to the Review into Open Banking in Australia, p. 14.

[11] The Australian Government the Treasury, 2017, *Review into open banking: giving customers choice, convenience and confidence*, p. 51.

[12] Deloitte 2018, *Open banking: A seismic shift*, p. 2; The Australian Government the Treasury, 2017, *Review into open banking: giving customers choice, convenience and confidence*, p. 60.

Table 2: Self-reported breaches of D23 Privacy, 2013–14 to 2016–17

	2013–14	2014–15	2015–16	2016–17
Breaches	**105**	**129**	**244**[13]	**294**[14]
In % of total breaches	*13%*	*20%*	*30%*	*24%*
Significant breaches	**1**	**2**	**5**	**0**

A further 11% of self-reported Code breaches in 2016–17 were breaches of the general obligation, under Key Promise 8, to comply with legal obligations (**Table 3**). Although data is not collected on which legal obligations were involved in these breaches, it is likely that a proportion of the 138 breaches of Key Promise 8 relate to Privacy Act obligations. This may include some double-counting if institutions self-reported the same breach under both obligations.

Table 3: Self-reported breaches of Key Promise 8, 2013–14 to 2016–17

	2013–14	2014–15	2015–16	2016–17
Breaches	**89**	**110**	**130**	**138**
In % of total breaches	*11%*	*17%*	*16%*	*11%*
Significant breaches	**2**	**1**	**2**	**0**

This high rate of non-compliance with privacy obligations has not been reflected in customer complaints to institutions, and indeed the Committee has not received any Code breach allegations regarding privacy. In 2016–17, only 1% of the internal dispute resolution (IDR) complaints recorded by institutions were related to privacy.

There has been no real increase in privacy-related IDR complaints in recent years. Interestingly, while nearly all large institutions self-reported privacy breaches in 2016–17, less than half self-reported any privacy complaints. Micro and small institutions, on the other hand, self-reported more privacy complaints and fewer breaches.

Institutions should proactively monitor their compliance with privacy obligations, rather than relying exclusively on customer complaints to identify issues.

This may suggest that micro and small institutions are relying too heavily on complaints to identify privacy breaches, rather than also conducting more proactive monitoring. While 24% of institutions reported non-compliance with legislative and Code privacy requirements, there are few complaints about privacy issues made to institutions.

[13] Two large institutions reported a quarter (60) of the total Code breaches regarding D23.

[14] One large institution reported a quarter (70) of the total Code breaches regarding D23.

Collecting personal information

Institutions may collect information that is reasonably necessary for them to carry out their functions or activities. In doing so, they are bound by APPs 3 and 4, which set out rules about how entities can collect solicited personal and sensitive information, and deal with unsolicited personal information.

Collection must be done fairly and lawfully and, where practicable, the information should be collected directly from the individual. Institutions must take reasonable steps to let individuals know why the information is collected, the identity of other institutions to which it may be disclosed and the fact that the individual can gain access to it.

Institutions should prevent the collection of unnecessary or irrelevant information.

Collecting only relevant information

All institutions reported that they have at least one mechanism to ensure that only necessary and relevant personal information is collected.[15] Institutions' primary means of preventing the collection of unnecessary or irrelevant information are staff procedures, which are employed by most institutions (90%) in each size category, although larger institutions are most likely to have such procedures in place.

Monitoring and quality assurance activities (58%) are also common, undertaken by more than half of institutions. Most commonly, institutions referred to internal or external audits, including branch audits. Institutions also cited random checks, call monitoring and routine observation of staff – particularly in micro institutions. Some institutions reported that hardcopy and online forms and other documentation are reviewed for privacy and compliance, including via hindsight reviews.

Several institutions also noted that their forms and systems only allow for the capture of necessary and relevant information. One small institution, however, explained that because its core banking system contains unnecessary fields, it needs to specifically train staff **not** to collect certain information.

Obtaining consent

Sensitive information, which includes information about a person's health or their professional and trade organisation memberships, is subject to additional protection under the APPs.

Institutions' responses indicated that sensitive information is only rarely required, such as when a customer includes health information in an application for financial hardship assistance or a consumer credit insurance claim, or where a medical questionnaire is completed as part of an application for a third-party travel insurance product. A handful of institutions stated that they never collect sensitive information as it is not required for any of their functions.

Institutions should have appropriate processes for seeking consent, preferably written consent for the collection of sensitive information.

Although consent is a fundamental concept underpinning the Privacy Act and the APPs, institutions are given considerable latitude in how they deal with consent in practice. At present, under the Privacy Act, consent can be express or implied. The Privacy Act does not prescribe how consent should be sought and provided.

Most commonly (78%), institutions reported that they seek written consent to collect sensitive information.[16] One-quarter (25%) of institutions rely exclusively on a written consent process, while an additional 55% combine a written consent process with other methods. Some institutions referred to a specific consent form or written authority, while others reported that consent is incorporated into membership and/or loan application forms, including online application forms.

Where sensitive information is required, a few micro and small institutions said that consent is treated as implied, as customers themselves provide the information. However, most institutions have a process for seeking explicit consent.

Most institutions also have a process for seeking verbal consent over the phone or in branches. Some 63% of institutions obtain consent verbally; this is the sole method of seeking consent for 7 institutions (10%), including some micro, small and large institutions. A couple of institutions commented that verbal consent is only used where written consent is not possible. One institution, however, noted that as part of its 'hardship approach', it seeks to minimise stress by relying only on verbal information, including verbal consent, for a member's first hardship assistance application.

Handling unsolicited personal information

Although a handful of institutions reported that unsolicited personal information is rarely or never received, most institutions do, on occasion, receive such information. For example, such information might be provided by another member or as part of a request from a government agency.

Institutions need processes and procedures for destroying unsolicited and unnecessary information.

[16] See Appendix 4, question 8.

Most institutions (75%) reported that they destroy unsolicited personal information.[17] Typically, they first assess the material to determine whether it is necessary and relevant, or whether it can be returned to the member. A few institutions, however, automatically consider unsolicited personal information or information that cannot be confirmed by the customer to be unnecessary or irrelevant and destroy it upon receipt as a matter of course.

Digital personal information that is not required is deleted by a clear majority (82%), with one institution noting that backup disks are also physically destroyed. Institutions destroy personal information in hard copy either by de-identifying it; shredding it and disposing of it securely; or blacking it out (if parts of the document are needed).

However, it should also be noted that approximately 30% of subscribers also advised that, when dealing with digital information that is no longer needed, they currently retain it indefinitely.

[17] See Appendix 4, question 9.

Managing personal information

Once information has been collected, the APPs and the Code set out a range of requirements for how that information is managed. Institutions have obligations to keep the information they hold secure, to maintain its accuracy and completeness, and to appropriately handle information that is no longer needed.

Maintaining security and integrity

Both the Code and the APPs place obligations on institutions to take 'reasonable steps' to maintain the security and integrity of personal information. Under APP 11, these steps must protect against 'misuse, interference and loss, and from unauthorised access, modification or disclosure'. Section 23.3 of the Code echoes this legal obligation, and additionally requires that institutions regularly review the security and reliability of their banking and payment systems.

Institutions should ensure that password protocols are strong and that staff never share passwords.

All institutions have a process in place to control employees' access to personal or sensitive information. For all large and most other institutions, these processes include banking system access restrictions.[18] Several institutions referred to information (such as TFNs) that is encrypted and/or entirely shielded from staff access. Access to information may be restricted by role, with some information visible only to management. Some institutions noted that they review access permissions as often as quarterly. Banking systems may also limit access with password protection, which in many cases leaves an auditable trail.

Many institutions combine these banking system access restrictions with manual control processes. Institutions reported that sensitive information in hard copy is kept in secured files or rooms with limited and logged access. As with information held digitally, access by staff is often restricted by role. One institution described its approach to managing access to sensitive hardship application information, most of which is kept in detailed manual records (rather than the core banking system) so that it can be destroyed easily once no longer needed.

Institutions should have a clean desk policy.

A handful of micro and small organisations rely on policies and procedures, training and/or manual checks and do not have any banking system restrictions. One commented that restricting access by role is impractical in a very small team of fewer than 10 employees, while another micro institution explained that although a recent system upgrade made it possible to hide sensitive information, this had not yet been implemented.

Institutions should ideally have banking system restrictions in place.

[18] See Appendix 4, question 16.

Most institutions have also taken several reasonable steps to protect information they hold from theft, unauthorised access, disclosure or loss.[19] The most common measure is staff training, which has been undertaken by all institutions.

All but one (large) institution reported that they had implemented electronic security systems, such as firewalls, anti-virus software and data encryption. Similarly, only one micro institution does not have data security measures in place.

Micro and small institutions are slightly less likely to have taken certain steps: a handful reported that they do not control access to their physical buildings; do not verify the identity of persons requesting information; and/or – as discussed above – do not place controls on staff access to information.

Institutions should have robust processes and procedures for verifying the identity of persons requesting access to personal information.

One micro and two large institutions do not have documented storage security policies and three micro, one small and one large institution do not place confidentiality requirements on staff. A couple of institutions noted that privacy and data security measures are also applied to contractors and subcontractors or other third parties.

Institutions should review the adequacy of their security arrangements at least annually.

Most institutions reported that they regularly or periodically review the adequacy of security arrangements for their banking and payment services. Just over half of all institutions (55%) review their security arrangements annually: this was the most common review frequency reported by institutions of all sizes.[20] A further 20% reported that they conduct such a review more than once per year. A few institutions review arrangements less frequently, such once every two or three years.

Some institutions said that their review of security arrangements is ad hoc, when necessitated by business requirements for different types of data; new legal or regulatory obligations; and security breach incidents either internally or at other institutions or companies.

New processes and technologies should prompt privacy impact and risk assessments before any third-party contractors are engaged.

A handful of institutions commented that they perform regular testing, such as monthly vulnerability scanning. While such testing is important, to meet the Code's Section 23.3 requirement, institutions must also regularly review the adequacy of their overall security approach.

Institutions should systematically review their privacy and security settings. This should include – but not be limited to – testing security settings.

[19] See Appendix 4, question 16.
[20] See Appendix 4, question 17.

Maintaining accuracy

In line with their obligations under APP10, all institutions reported that they take reasonable steps to ensure that the personal information they collect is accurate, up-to-date, and complete.[21]

Staff at most (74%) institutions also manually review information before or after collection, use and disclosure. Regular system or systematic review to verify the accuracy of data was the third-most commonly used measure, employed by 42% of institutions.

Fewer than one in 10 institutions (7%) update information provided by unauthorised or unrelated third parties. One institution noted that it also investigates statements that are returned to sender to update customer information.

Manual reviews and spot checks should be supplemented by regular system-wide reviews of data accuracy. Where appropriate, they should use information from third parties and other sources to update customer information.

All but four (micro and small) institutions said that they update information once notified of corrections or updates by the customer or a third party. Some institutions made additional comments noting that they proactively seek this information from customers, for example as part of standard telephone contact procedures, reminders in regular newsletters or periodic 'campaigns' requesting updates.

Where a customer contacts an institution to update their details, the Code requires that the correction be made 'promptly'. Although the time taken to make corrections may vary with the complexity of the information, nearly half of institutions (49%) reported that such corrections are typically made within 24 hours,[22] with micro institutions most likely (67%) to adhere to this timeframe. A further 15% of institutions define 'promptly' as within 48 hours.

At times, institutions themselves become aware that personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, without being notified of this by the customer.

For example, an institution may detect that a phone number has been disconnected. Where this occurs, institutions take reasonable steps to confirm and correct the information they hold.

Institutions should take reasonable steps to confirm and correct information, including contacting customers. They should check that inaccurate, out-of-date, incomplete, irrelevant or misleading information has not impacted the customer or third parties before removing it from the system.

[21] See Appendix 4, question 14.
[22] See Appendix 4, question 15.

Almost all institutions (97%) reported that they contact the customer to update the information.[23] Most (77%) then remove inaccurate, out-of-date, incomplete, irrelevant or misleading information from their systems.

Four in 10 institutions (40%) contact any third parties to whom this information has previously been disclosed, and one-third (33%) make updates based on information from third parties, probably because unsolicited personal information is often destroyed (see discussion on p. 14).

Managing unneeded information

Institutions should have processes to ensure that information that is no longer needed is destroyed or de-identified.

Except for one large institution, all institutions said that unneeded hard copy documents are securely destroyed.[24] In comments, a few large institutions explained that they have a Records Retention Schedule or Information Retention Standard, which sets out when documents of different types are to be securely destroyed after a period of archiving. A substantial minority of institutions (40%) retain but de-identify hard copy documents that are no longer needed, with large institutions more likely to take this step (60%). A quarter of institutions (25%) will return hard copy records to customers – something that may only be done upon customer request.

Regarding digital information, the most common approach – reported by four in five institutions (82%) – is to securely destroy data that is no longer needed.[25] As with paper-based records, this destruction may be carried out according to a Records Retention Schedule.

Institutions should have a policy and processes for destroying or de-identifying unneeded information, including digital information.

However, a quarter of large institutions (25%), as well as a few micro, small and medium institutions, reported that they do not destroy digital data. Instead, such data is retained indefinitely, but made inaccessible to most or all staff. Only one in three institutions (28%) de-identify digital information, and just two small institutions (3%) return digital information to customers when it is no longer needed.

A few institutions commented that they have no policy or procedure covering de-identification or destruction of digital information. To address these gaps, three institutions were currently considering or developing procedures in this area.

[23] See Appendix 4, question 25.
[24] See Appendix 4, question 19
[25] See Appendix 4, question 20

Using personal information

The advent of open banking will see personal information opened up to new uses by a wider range of third parties. This will bring added complexity to the management of personal information and make it even more important for institutions to have rigorous and effective procedures for managing disclosure. Ahead of these changes, institutions should ensure that they are complying with their existing APP obligations regarding the use of personal information that they hold.

Institutions should ensure their privacy procedures cover how information can be used for direct marketing and when it can be disclosed to other parties, as well as how customers can access their own data.

Direct marketing

Under the requirements of APP 7, institutions can only use or disclose personal information for direct marketing under certain conditions. One of these conditions is that individuals are given a simple means of opting out of direct marketing communications. Institutions must also act on an individual's request that their personal information not be used or disclosed for direct marketing purposes.

All institutions reported that they accept such requests, and most accept requests via multiple channels. Most commonly, 93% of institutions reported that they accept written requests.[26] Almost as many (90%) will act on verbal instruction from the customer. Twenty institutions (30%) offer a paper request form and almost as many (25%) have an online form for customers to opt out of any direct marketing. It appears that some institutions offer quite narrow avenues for customers wishing to opt out, for example, requiring that they visit a branch or contact the institution's Privacy Officer. Other institutions commented that they will accept and act on a customer's request however it is received. This makes it easy for customers to opt out and represents good practice.

Almost all institutions that send direct marketing information to customers[27] include an opt-out statement in each such communication. In electronic direction mail (EDM) communications, institutions include an 'opt out', 'unsubscribe' or 'update preferences' link in the footer, often together with a statement and/or a link to the institution's privacy policy. SMS communications include an opt-out reply instruction. In letters, institutions reference their privacy policies and provide contact details with instructions for those who wish not to receive future marketing material.

[26] See Appendix 4, question 12

[27] Five micro institutions reported that they do not send any direct marketing to members.

Note that under the Spam Act 2003 every commercial electronic message must contain an unsubscribe facility. Further to this, commercial electronic messages must only be sent with consumer consent however inferred consent can be relied upon when sending electronic messages to existing customers.

It is the Committee's view that all institutions should include opt-out options for all forms of direct marketing material – electronic or otherwise.

Institutions should follow good practice by making direct marketing an opt-in choice. At a minimum, they must have clear, plain English avenues for opting out.

Only four institutions – all of them micro – said that they do not include an opt-out.[28] One was in the process of implementing an opt-out at the time of the inquiry, while two reported that they only include occasional marketing information enclosed with statements.

Disclosing personal information

Rules about disclosing personal information – that is, passing it outside the institution – are contained in APP6. Institutions can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. Code Section 23.2 further requires that institutions not disclose personal or financial information unless:

- required to do so by law
- there is a duty to the public to disclose the information
- the institution's interests require disclosure (for example, to prevent fraud)
- the customer asks the institution to disclose the information
- the customer gives permission for the institution to disclose the information.

Although oral consent is sufficient, institutions often ask customers to sign a privacy consent, giving permission for the institution to disclose personal information in certain circumstances. Most often, privacy consents are used as part of loan applications. Institutions have different ways of seeking to ensure that customers understand these privacy consents before signing. Positively, many institutions reported that staff explain privacy consents to customers before signing, inviting questions.

Institutions should specifically develop privacy consents to support understanding, using concise, plain English expression and user-friendly design.

[28] See Appendix 4, question 13

The discussion may include an explanation of why the information is needed. Often, the discussion occurs as a matter of course (and may be scripted); in other cases, staff have discretion to judge whether the customer seems to understand or requires additional explanation.

One institution noted that interpreters are made available for this discussion if required. Somewhat less proactively, some institutions respond to but do not invite customer questions about privacy consents.

Institutions often explicitly instruct customers to read the document and may advise them that they can take time to consider it or seek advice from a lawyer or support person. The customer may then be asked to confirm that they have read and/or understood the privacy consent before agreeing to it.

A few institutions specifically noted that they do not accept privacy consents from any individual who does not have the capacity to consent. At the other end of this spectrum, and disappointingly, a few micro and small institutions reported that they assume understanding and take no steps to support or confirm it.

The advent of open banking is likely to impact on how consent is treated in the Privacy Act and managed by institutions. In line with concerns expressed by many stakeholders, including COBA,[29] the Farrell Review concluded that the breadth of consent in the Privacy Act is too broad for the open banking environment.

To ensure that customers understand what they are agreeing to, consent in the open banking environment will need to be more meaningful: freely given; expressed, not implied; informed; specific as to purpose; time-limited and able to be easily withdrawn with immediate effect.

Institutions should review their privacy consent processes considering open banking requirements.

Pleasingly, it seems that some institutions have already instituted processes to ensure that customers' consent meets a number of these criteria.

Those institutions that merely assume customer understanding, however, should begin considering how they can revise their consent processes to be more meaningful.

Advising customers that their information has been disclosed

[29] Customer Owned Banking Association, 29 September 2017, Submission to the Review into Open Banking in Australia.

As well as seeking customer consent in advance, institutions may advise customers that they have disclosed personal information for the purposes set out in Section 23.2 of the Code.

Most commonly, this is done in writing (64% of institutions).[30] Half (51%) tell the customer verbally and 34% do so online. Several institutions noted that where consent had already been provided or the reasons for disclosure set out in the Privacy Policy, they would generally not advise customers of specific disclosures thereafter – particularly where, for example, the disclosure related to fraud prevention. One institution reported that it may tell a customer about a disclosure in response to a query from the customer.

Providing customer access to information

Under APP12, upon request institutions must give customers access to information held about them, unless a specific exception applies. Section 23.4 of the Code echoes this legal obligation. APP12 also sets out various requirements as to when and how access is to be provided or refused.

To comply with APP12, institutions must respond to a customer's request for access within a reasonable period, which should generally not exceed 30 days.

A majority of institutions (58%) reported that on average, they respond to customer requests within 5 days.[31] Others commented that while timeframes vary based on the nature of the request, most are responded to immediately (once identity has been verified as required by the Privacy Act). A further 10% of institutions respond, on average, within 30 days. Several micro institutions commented that they had never received a customer request for access to personal information or received them only very rarely.

If access is refused, APP12 requires that institutions provide a written notice of the refusal which must include the reason for the refusal.

Most (61%) organisations said that they do provide such a written notice.[32] Most of the remaining institutions indicated that they had never had occasion to refuse a customer's request for access, but that they would provide the reason for refusal in writing were it to occur. A couple reported that they would not refuse a customer's request.

Institutions should develop processes for providing written refusal of a customer's request for access to information.

[30] See Appendix 4, question 11
[31] See Appendix 4, question 21
[32] See Appendix 4, question 22

Comments from a handful of institutions indicated that they may not be aware of the APP requirement for written notice of refusal and the reason for it.

One micro institution reported that it had never refused a request but that if it did, it would provide the reason for refusal 'if necessary'. One small institution commented that it would offer a verbal explanation of the reason for refusal and only provide this in writing if asked by the customer to do so; one large institution recounted an instance of a refusal being dealt with in this manner. One medium institution said that it did not have a documented procedure but would follow its ordinary complaint handling process.

Given that there are legitimate reasons a request may be refused, institutions should have a process for providing written notice of such refusal.

The survey provided inconsistent data on whether institutions charge fees for customers to access their own information. The APPs specify that institutions may charge a fee for providing a customer with access to their information, providing this fee is not excessive and does not apply to the making of the request.

When a guarantor requests information about a customer, institutions most often provide information about the debtor's loan amounts that are overdue and the dates they became due (81%),[33] the debtor's loan balance (79%), and their loan payment history (70%).

A handful of institutions (12%) will provide the debtor's combined loan, savings and transactional account statements. Many institutions commented that they will provide a range of other information, including net asset/liability position; annual income; the credit contract, guarantee and indemnity; payout figures; details of any security held, and so on.

These responses indicate that many institutions have a poor understanding of privacy requirements concerning information disclosure to guarantors.

Under s 36 of the National Credit Code, once the loan is established institutions should only provide information to a guarantor that directly relates to the current loan, such as the current balance of the debtor's account; any amounts credited or debited during a specified period; any amounts currently overdue and the dates they became due; and any amount currently

Institutions should review their compliance with privacy requirements on information disclosure to guarantors. They should only provide information concerning the loan, including the current balance of the debtor's account; any amounts credited or debited during a period specified in the request; any amounts currently overdue and the dates they became due; and any amount currently payable and the date it becomes due. They must not provide information about a customer's transaction or savings accounts.

[33] See Appendix 4, question 24

payable and the date it becomes due. Institutions should not disclose information about a customer's transactional or savings accounts; this constitutes a privacy breach.

Prior to approving a loan, institutions should provide the guarantor with the Information Statement Things You Should Know About Guarantees, the Prescribed Warning (Form 8) and any additional information institutions have that a careful and prudent prospective guarantor may wish to consider regarding the financial position of the borrower and the borrowers credit history for the previous 12 months. Institutions are required to gain the borrower's prior consent to release this information.

Managing compliance with privacy obligations

Reiterating institutions' legal obligations, the Code specifically requires that institutions comply with the *Privacy Act 1988* and the APPs. While compliant systems, policies and procedures are important, staff training is critical to translating these into compliant practice. Even when compliance is achieved, to maintain it over time, institutions must periodically review their compliance frameworks – particularly as the industry context and the legislative and regulatory framework continue to evolve.

Training staff

Training staff to understand their legal and Code obligations and to work in line with both is essential to compliance.

All institutions take steps to train staff in Code requirements, either face-to-face or via e-learning. For most institutions, in-house training (87%) and discussion in staff meetings (70%) are the centrepiece of training efforts.[34] A smaller group of institutions (33%) provide external training, either exclusively or alongside in-house training.

Often, training and discussion are complemented with written material including information sheets (39%) and content placed on staff intranets (49%). These same means are used to make staff aware of any privacy breaches or complaints that have occurred within the institution. The specific modules staff receive may be aligned to their role.

Even so, the clear majority of institutions (93%) train **all** staff in compliance with the Code's privacy obligations (Section D 23), regardless of role. Two medium and one micro organisation only train customer facing staff in privacy obligations.[35]

Even though all institutions have training programs and processes in place, the high proportion of privacy breaches caused by human error or a failure to follow established processes suggests that more can be done to create a strong culture of privacy compliance.

Institutions report that more than three-quarters of breaches (76%) occur when personal information is mistakenly released due to human processing error, with one in ten institutions reporting that this occurred at least once in the last month. In large institutions, staff have also released personal information because insufficient training left them unaware of privacy obligations.

Institutions should provide ongoing and refresher training, as well as routine staff alerts and reminders of privacy obligations to all staff that have contact with customer personal information.

[34] See Appendix 4, question 27.
[35] See Appendix 4, question 26.

Reviewing compliance

Institutions have different ways of reviewing their compliance with the *Privacy Act*. Many conduct regular, scheduled privacy compliance reviews.

Institutions should conduct a comprehensive privacy review annually.

For some institutions, these reviews appear to address their privacy policies only, while other institutions' review processes are more holistic, encompassing privacy notices and procedures, privacy management statements and systems, and related training and complaints processes.

Other institutions reported that they review privacy compliance on a more ad hoc or ongoing basis, often but not always in addition to scheduled reviews.

Ad hoc review may be prompted by business changes, including system upgrades or process changes; by a breach or incident that alerts the institution to an issue; or by amendments to the Privacy Act or Principles such as the open banking changes that have been recommended by the Farrell Review.[36]

Several institutions described their processes for staying up-to-date with legislative and regulatory change via external legal advice or subscriptions to compliance news such as updates from the Office of the Australian Information Commission (OAIC) and COBA compliance notes.

Through some or all these methods, most institutions reported that they fully or partially review their compliance with the *Privacy Act 1988* at least annually.[37]

Institutions should ensure that there are strict contractual Service Level Agreements in place with all third-party suppliers that have access to customer information and that these are regularly monitored of performance against the agreed SLAs. Examples of third parties include customer statement printers, IT software providers, external help desks, auditors, etc.

Privacy policies

Under APP1, which concerns open and transparent management of personal information, entities must have a clear and up-to-date privacy policy. The Code specifies that institutions must make such privacy policies available on request and publish them on their websites.

All institutions have a comprehensive privacy policy, often based on COBA templates. With only one exception, all institutions reported that their privacy policies cover each of the required information types, namely:[38]

- the kinds of personal information that the institution can collect and hold
- how they collect and hold personal information

[36] See recommendations in Chapter 4, The Australian Government the Treasury, 2017, *Review into open banking: giving customers choice, convenience and confidence*.
[37] See Appendix 4, questions 2 and 3.
[38] See Appendix 4, question 5.

- the purposes for which they collect, hold, use and disclose personal information
- how a customer may access personal information about themselves held by the institution, and seek correction of such information
- how a customer may complain about a breach, and how the institution will deal with such a complaint.

Some institutions also noted that their privacy policy addresses how they will deal with overseas disclosures.

Institutions should review how they deal with overseas disclosure.

Institutions reported that they make their privacy policies easily available to customers and potential customers. All institutions reported that their privacy policies are available on their websites.[39]

Most institutions (90%) will also supply their privacy policy via mail or email upon request, while more than half also include it in communications to new members, either in full or abbreviated. Only one-third of institutions (34%) will read the privacy policy out to customers, with large institutions most likely to offer this service.

Other ways in which some institutions provide the Privacy Policy are via hard copies in branches, through links within online loan application forms, or via a pre-recorded message when customers phone in.

Institutions should ensure that their privacy policies are visible and readily accessible to customers.

[39] See Appendix 4, question 4.

Conclusion

Privacy and data security is a crucial area of compliance for customer owned banking institutions, and the importance and complexity of these obligations is only increasing. In this context and given the relatively high level of non-compliance with existing privacy obligations, the Committee determined that it was important to conduct an in-depth investigation into institutions' privacy compliance.

This inquiry found that although institutions' documented privacy policies and processes appear to be compliant and available to customers, improvements are needed to staff training and in specific areas, such as disclosures to guarantors. Procedures for collecting personal information and obtaining consent to this collection need to be reviewed, with thought given to future open banking requirements. Similarly, institutions can further improve their processes to control employee access to personal or sensitive information and protect it from theft, unauthorised access, disclosure or loss.

Although policies and procedures are largely compliant in general, the frequency of breaches resulting from human error suggests that policies and procedures are not always successfully translated into compliant practices. Institutions report that 76% of privacy breaches involve the mistaken disclosure of personal information because of human error. This underscores the importance of both training staff in privacy requirements and reiterating these obligations and their importance with refresher training and other reminders.

There is also evidence of some systems-related privacy issues. The Committee's ACS Verification Program[40] uncovered instances of privacy breaches due to systems errors, often associated with banking platform transfers or upgrades.[41]

In some cases, systems failure and human error can interact. For example, one breach occurred when a system upgrade increased call volume, leading to incorrect data entry. For this inquiry, one institution reported that it trains staff not to collect unnecessary data requested by the core banking system. Any staff error in such a circumstance might equally be considered a systemic failure or human processing error.

In some areas, several institutions are technically compliant but falling behind in terms of good practice. While most of institutions enable customers to opt-out of direct marketing communications, this process could often be made easier for consumers.

---

[40] See p. 10

[41] See Customer Owned Banking Code Compliance Committee (May 2018) *Managing Privacy Compliance: Lessons from the ACS Verification Program*.

Similarly, although institutions seek consent before disclosing personal information, only some take steps to ensure that consent is meaningful, and customers understand what they are agreeing to. Continued complacency in areas such as these could mean that these institutions will be ill-prepared for the challenges that institutions will face as open banking transforms the financial services sector.

To improve compliance with current Code obligations and to prepare for the future, the Committee believes that all institutions could benefit from comprehensively reviewing their privacy and data security policies and practices.

Checklist 1 below identifies some of the source materials that should underpin such as review, while checklists 2–5 and 7 identify some key areas for consideration. Checklist 11 covers embedding change in the institution's policies and procedures. Checklist 8 focuses on training staff to ensure compliance in practice, while Checklist 6 focuses on maintaining compliance with regular spot checks. Protecting privacy in arrangements with third parties – an issue that will become increasingly crucial in any future open banking regime – is addressed in checklists 9 and 10.

Privacy compliance checklist

1. Review privacy source materials.

Source materials for review include:

- Office of the Australian Information Commissioner (OAIC) guides such as *A Guide to Handling Personal Information Security Breaches*
- COBA's *Record Retention – a Guide to your Legal Obligations* (May 2016)
- COBA's *Australian Privacy Principles Compliance Manual* (February 2018)

2. Review your privacy policy, privacy notification and process for obtaining consent.

- Is your Privacy Policy easily available to customers and potential customers?
- Ensure both your hard copy and online customer application processes include your Privacy Notification.
- Consider use of a standard privacy oral consent script and/or a pre-recorded message to capture the first time you talk to potential customers.
- Does your Privacy Policy address how you deal with overseas disclosures?

3. Review data security and integrity.

- Review staff access levels to the banking system and internal documents regularly, ideally annually. Are they up to date and consistent with all job descriptions?
- Is your password protocol strong and are you sure that staff never share passwords?
- Have you conducted an audit on the physical access at all locations?

4. Review retention and deletion/de-identification of personal information.

- Review your retention practices for both soft and hard copy documents for each department. Do you have processes and procedures in place to ensure that all information is destroyed and/or de-identified when no longer required?
- Review any off-site storage and scanning processes. Do you have destruction protocols in place?

5. Review breaches and determine trends and additional controls.

- Review your incident and breach register and look for privacy breach trends. Are there any controls that can be added to reduce recurrence?
- Review the last COBCOBP Annual Report breaches – can you learn any lessons from other's experiences and remediation plans?

6. Review compliance with privacy spot checks.

- Do you have regular privacy reviews scheduled? Has a review been conducted within the last two years?
- Conduct a clean desk policy sweep of all business locations. Is any personal information left in plain sight? Remember to check waste bins and all public areas.
- Make some shadow shopping calls. Are staff in all front-line situations following your privacy notification requirements for new and potential customers?
- Does your website include the current versions of your Privacy Notification and Policy? Are they easy to find?
- Check your TFN retention processes. Is access restricted to staff whose role specifically requires access?
- Do you always include an opt-out option on any customer direct marketing material you distribute electronically?
- How do your staff handle a loan balance request from a guarantor?

7. Ensure you have a compliant Data Breach Response Plan (DBRP).

- Ensure you have privacy and data breach roles and responsibilities clearly defined within a Board-approved policy.
- Have a clear escalation process that staff can refer to (a flow chart is a good visual guide).
- Ensure your DBRP caters for both large scale cyber interruption and individual customer data breaches.
- Ensure your DBRP includes your process to report to the OAIC and how you will notify individuals at serious risk of a data breach.

8. Raise staff awareness of privacy requirements and your DBRP.

- Implement a staff training program that includes how to identify a data breach, how to minimise potential data breaches and how to report data breaches.
- Ensure your annual privacy training material is updated to include questions to test staff knowledge and understanding of the DBRP.
- Consider using a mix of formal and informal training methods – face-to-face, e-learning, in-house and external training sessions, intranet resources, staff meetings, reminder emails and quizzes.
- Consider what other ways you can embed compliance with privacy obligations into your company's risk framework.

9. Consider your third-party contracts.

- Are the privacy and data breach reporting clauses sufficient?
- Are you comfortable with the third-party access to customer personal information and their data security arrangements?
- Are you regularly monitoring performance against the agreed Service Level Agreements?

10. Ensure that new processes and technology are privacy compliant.

- Ensure you conduct a privacy impact and risk assessment prior to engaging with third-party contractors or services that include exposure to customer's personal information.

11. Embed changes into your relevant policies and procedures.

- Following the outcomes of the steps above update the appropriate policies and procedures, including (but not limited to):
    - Privacy Program, Policy and Notifications
    - Staff Training Policy and Programs
    - Business Continuity Plan and Policy
    - Data Breach Policy
    - Outsourcing Policy
    - Incident Management Policy
    - Customer Complaints Policy

Appendix 1: Online questionnaire

A Compliance with privacy obligations (D23.1, D23.5)

23.1. We will comply with the Privacy Act 1988 and the APPs, including with respect to credit reporting and the collection, storage, use and disclosure of your personal and financial information.

23.5 We will make a copy of our Privacy Policy available to you on request and will publish it on our website, if we have one. We will tell you about our Privacy Policy if you ask us.

Institutions must comply with the APPs, which form a schedule to the Privacy Act 1988. From 12 March 2014, the APPs set the minimum standard for the collecting and handling of personal information.

1. How does your institution review its compliance with the Privacy Act 1988 and the APPs? *(Please comment)*

2. How often does your institution review its compliance with the Privacy Act 1988 and the APPs, including with respect to credit reporting and the collection, storage, use and disclosure of personal and financial information? *(Please select ONE only and provide comment)*
   - ☐ Quarterly, please comment
   - ☐ Semi-annually, please comment
   - ☐ Annually, please comment
   - ☐ Biennially, please comment
   - ☐ Other, please comment

3. When was your last privacy compliance review? *(Please select ONE only)*
   - ☐ Within the last six months
   - ☐ Within the last year
   - ☐ Within the last 18 months
   - ☐ More than two years ago
   - ☐ Other, please comment

4. How do you make your Privacy Policy available to your customers as per Section D23.5? *(Please select ALL that apply)*
   - ☐ On website
   - ☐ Sent by mail/email upon request
   - ☐ As part of regular documents sent out to customers (e.g. new member packs)
   - ☐ Verbally
   - ☐ Other, please comment

5. Does your Privacy Policy contain the information listed below?
   (Please select ALL that apply)
   - ☐ The kinds of personal information that you can collect and hold
   - ☐ How you collect and hold personal information
   - ☐ The purposes for which you collect, hold, use and disclose personal information
   - ☐ How a customer may access personal information about the customer that is held by you, and seek correction of such information
   - ☐ How a customer may complain about a breach, and how you will deal with such a complaint
   - ☐ Other, please comment

B Consideration of personal information privacy (APPs 1 to 2)

APP 1 — Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

Personal information is any information about an individual whose identity is apparent or can reasonably be ascertained. It includes an opinion or evaluative material. Even if the information is not true, it is protected if it relates to an identifiable individual.

Sensitive information is subject to additional protections under the APP due to the nature of this information.

6. How do you control employee access to identify personal or sensitive information?
   (Please select ALL that apply and provide comments)
   - ☐ Manually, please comment
   - ☐ Banking system access restrictions, please comment
   - ☐ We do not have a process, please comment
   - ☐ Other, please comment

C Collection of personal information (APPs 3 to 5)

APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

An institution can collect information that is reasonably necessary for one or more of its functions or activities. Collection must be done fairly and lawfully and, where practicable, the information should be collected directly from the individual.

Institutions must take reasonable steps to let individuals know why the information is collected, the identity of other institutions to which it may be disclosed and the fact that the individual can gain access to it.

7. How does your institution determine that the personal or sensitive information that you collect is reasonably necessary, or directly related to, one or more of your functions or activities?
   (Please select ALL that apply and provide comment)
   - ☐ Staff Procedures, please comment
   - ☐ Independent monitoring & assurance activity, please comment
   - ☐ Review of customer information held, please comment
   - ☐ Staff controls, please comment
   - ☐ Other, please comment

8. How do you seek consent from your customers before collecting sensitive information about the customer if the information is reasonably necessary, or directly related to, one or more of your functions or activities?
   (Please select ALL that apply and provide comments)
   - ☐ Seek consent verbally, please comment
   - ☐ Seek consent in writing, please comment
   - ☐ Other, please comment

9. Describe your process for managing and/or handling unsolicited personal information (e.g. member information received from another member or government agency requests)?
   (Please select ALL that apply and provide comments)
   - ☐ Determine if you could or could not have collected the personal information, please comment
   - ☐ Determine if the information is necessary, please comment
   - ☐ Destroy the information if practicable, please comment
   - ☐ De-identify the information if practicable, please comment
   - ☐ Other, please comment

D Dealing with personal information (APPs 6 to 9, D23.2)

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual.

23.2 We will treat your personal and financial information as private and confidential. We will not disclose that information to any other organisation unless:

- we are required to by law (for example, under anti-money laundering laws)

- there is a duty to the public to disclose the information

- our interests require disclosure (for example, to prevent fraud)

- you ask us to disclose the information, or

- we have your permission to do so.

Principle 6 deals with the use and disclosure of personal information. Use means handling of that information within the institution. Disclosure means passing it outside the institution.

The Principles also differentiate between Primary Purpose and Secondary (related) purpose.

Commercial enterprises market products and are permitted to collect information to source new customers and contact them. There are additional restrictions on cross-border disclosure in Principle 7.

10. A customer may sign or acknowledge a privacy consent when prompted from your institution. What actions or activities do you undertake to ensure the content of the consent is understood by the customer? *(Please comment)*

11. How do you advise your customer that you have disclosed private and confidential information to another party as per exemptions listed in Section 23.2?
(Please select ALL that apply)
    - Verbally
    - In writing
    - Online
    - Other, please comment

12. How may a customer request not to receive direct marketing communications?
(Please select ALL that apply)
    - Verbally
    - In writing
    - Opt-out upon receipt of an electronic communication from your institution
    - Completion of an online form
    - Completion of a paper form
    - Other, please comment

13. In each direct marketing communication with the customer, do you include an opt-out statement or other clause to inform the customer how they can make a request to not receive direct marketing communications?
(Please select ONE only and provide comments)
    - Yes, rely on a general “click here for our privacy policy” in disclaimer
    - Yes, other, please comment
    - No, please comment
    - Other, please comment

E Integrity of personal information (APPs 10 to 11, D23.3, D23.4)

APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

23.3. We will take reasonable steps to protect your personal and financial information from misuse or loss, and from unauthorised access, modification or disclosure. We will regularly review the security and reliability of our banking and payment services.

23.4. We will give you access to the information we hold on you if you ask us to, subject to certain exceptions. These are set out in our Privacy Policy and are consistent with the APPs. We will correct any error that you bring to our attention. If your details change, tell us as soon as possible — we will update our records promptly.

14. What reasonable steps does your institution undertake to ensure that information they collect, use or disclose is complete, accurate and up-to-date?
(Please select ALL that apply)
    - ☐ Manual review of information by employees before or after collection, use and disclosure
    - ☐ Automated review of information collected
    - ☐ Updating information once notified by the consumer or authorised third party
    - ☐ Updating information provided by unauthorised or unrelated third parties
    - ☐ Regular system or systematic review of data held to verify its adequacy
    - ☐ Other, please comment

15. How do you define ‘promptly’ when updating errors brought to your attention by your customer regarding information held by your institution as per Section 23.4?
(Please select ONE only)
    - ☐ Within 24 hours
    - ☐ Within 48 hours
    - ☐ Within one week
    - ☐ Not defined
    - ☐ Other, please comment

16. What reasonable steps has your institution undertaken to ensure that information they hold is protected from theft, unauthorised access or disclosure and loss?
(Please select ALL that apply)
    - ☐ Document storage security policies
    - ☐ Controlled access to our physical buildings
    - ☐ Verifying the identity of the individual requesting the information
    - ☐ Data security measures
    - ☐ Electronic security systems, such as firewalls, virus software and data encryption on your website
    - ☐ Limiting access to employees on a needs basis
    - ☐ Confidentiality requirements of employees
    - ☐ Staff training
    - ☐ Other, please comment

17. How often do you review the adequacy of security arrangements of your banking and payment services to protect personal and financial information from misuse, loss or unauthorised access modification or disclosure as per Section 23.3?
(Please select ONE only)
    - Quarterly
    - Semi-annually
    - Annually
    - Biennially
    - Other, please comment

18. When was your last review regarding the security and reliability of your data?
(Please select ONE only)
    - Within the last six months
    - Within the last year
    - Within the last 18 months
    - More than two years ago
    - Other, please comment

19. What reasonable steps has your institution undertaken to deal with **paper-based** information when these are no longer required for any purpose?
(Please select ALL that apply)
    - Returning documents to the customer
    - Destroying documents in a secure manner
    - De-identifying the documents
    - Other, please comment

20. What reasonable steps has your institution undertaken to deal with **digital data** information when these are no longer required for any purpose?
(Please select ALL that apply)
    - Returning data to the customer
    - Destroying data in a secure manner
    - De-identifying the data
    - Other, please comment

F Access to, and correction of, personal information (APPs 12 to 13)

APP 12 — Access to personal information

Outlines an APP entity's obligations when an individual request to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

21. What is the average timeframe for your response to a customer's request for access to their personal information? *(Please select ONE only)*
    - Within 5 days
    - Within 30 days
    - Within 45 days
    - Over 45 days
    - Timeframe not measured/captured
    - Other, please comment

22. If you refuse to provide access to personal information, do you provide the consumer a written notice stating the reasons for the refusal and the mechanisms available to complain? *(Please select ONE only and provide comments)*
    - Yes, please comment
    - No, please comment
    - Other, please comment

23. Do you charge a fee to customers who request access to their personal information? *(Please select ONE only and provide comments)*
    - Yes, please comment on the average amount charged pre-request and the number of requests received
    - No, please comment
    - Other, please comment

24. What information do you provide to a loan guarantor on request? *(Please select ALL that apply)*
    - The debtors combined loan, savings and transactional account statements
    - The debtors loan payment history
    - The debtors loan balance
    - The debtors loan amounts that are currently overdue and dates they became due
    - Other, please comment

25. What reasonable steps does your institution undertake to correct personal information if it is inaccurate, out-of-date, incomplete, irrelevant or misleading? *(Please select ALL that apply)*
    - Contacting the relevant customer to update the information
    - Updating the information with more accurate, up-to-date, complete or relevant information from third parties

- Removing the information from your system once detected as being inaccurate, out-of-date, incomplete, irrelevant or misleading
- Contacting all relevant third parties whom you have disclosed the inaccurate, out-of-date, incomplete, irrelevant or misleading information to
- Other, please comment

G Training (Key Promise 8)

'We will comply with our legal and industry obligations.

We will be responsible, prudent managers of our institution, and will comply with all our obligations under the law and relevant codes of practice. We will act fairly and consistently with good banking and financial service industry practice.'

26. Do you train all staff regardless of position in compliance with Section D23?
    (Please select ONE only)
    - Yes, all staff receive training regardless of position or interaction with customers
    - No, only customer facing/advice giving staff receive training
    - Other, please comment

27. How do you train staff in compliance with Section D23?
    (Please select ALL that apply)
    - In-house training
    - External training
    - Staff meetings
    - Staff information sheets
    - Intranet
    - Other, please comment

28. How do you make staff aware of any breaches/complaints that occurred within your institution concerning Section D23?
    (Please select ALL that apply)
    - In-house training
    - External training
    - Staff meetings
    - Staff information sheets
    - Intranet
    - Other, please comment

H Information regarding privacy breaches and complaints

29. Please rate the following issues and main causes as the most likely to have occurred in your business. *(use rating scale from 0 – 5:*

    0 never happened
    1 has occurred at least once in the last 36 months+
    2 has occurred at least once in the last 24months
    3 has occurred at least once in the last 12 months
    4 has occurred at least once in the last 6 months
    5 has occurred at least once in the last month

- Human processing error (individual releasing the personal information of another person by mistake)
- Insufficient training (individual releasing the personal information of another person due to lack of knowledge in privacy obligations)
- Third party provider error (such as mail house mistakenly sending details out to the wrong address)
- Technical error (system mistakenly providing personal information to the wrong person)
- Unauthorised access (employees accessing or disclosing personal information outside the requirements or authorisation of their employment)
- Malicious actions (such as data theft or 'hacking')
- Other, please comment

30. What percentage of breaches or incidents relating to Privacy are systemic in nature? (*Please comment)*

31. Please advise how often remedial action has been required in response to a Privacy breach or complaint within your institution, and what that remediation activity has included. *(Please advise numbers and commentary if necessary)*
    - Minor – Customer request/access granted / data corrected / Staff Feedback
    - Moderate – Apology / Acknowledgement of error/ Staff Training / Procedure Change
    - Significant – Multiple or Systemic Customer Remediation / Report to Regulator / Business Continuity Crisis Management
    - Other, please comment

32. What do you think are the main causes of the current high number of privacy breaches reported within the customer owned banking sector?

Appendix 2: Australian Privacy Principles

APP 1 — Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information

Outlines an APP entity's obligations when an individual request to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

Appendix 3: Code obligations

Section D23

23.1. We will comply with the Privacy Act 1988 and the APPs, including with respect to credit reporting and the collection, storage, use and disclosure of your personal and financial information.

23.2 We will treat your personal and financial information as private and confidential. We will not disclose that information to any other organisation unless:

- we are required to by law (for example, under anti-money laundering laws)
- there is a duty to the public to disclose the information
- our interests require disclosure (for example, to prevent fraud)
- you ask us to disclose the information, or
- we have your permission to do so.

23.3. We will take reasonable steps to protect your personal and financial information from misuse or loss, and from unauthorised access, modification or disclosure. We will regularly review the security and reliability of our banking and payment services.

23.4. We will give you access to the information we hold on you if you ask us to, subject to certain exceptions. These are set out in our Privacy Policy and are consistent with the APPs. We will correct any error that you bring to our attention. If your details change, tell us as soon as possible — we will update our records promptly.

23.5 We will make a copy of our Privacy Policy available to you on request and will publish it on our website, if we have one. We will tell you about our Privacy Policy if you ask us.

23.6. Subject to applicable laws, the commitments made in this section do not prevent us from disclosing personal and financial information to other companies in a group of companies that we belong to (where applicable).

23.7. We will comply with all applicable laws relating to the retention of your personal and financial information.

Key Promise 8

We will comply with our legal and industry obligations.

We will be responsible, prudent managers of our institution, and will comply with all our obligations under the law and relevant codes of practice. We will act fairly and consistently with good banking and financial service industry practice.

Appendix 4: Questionnaire results

Definitions of institutions based on $ amount in assets:

- 27 micro institution: less than $200m in assets
- 10 small institutions: between $200m to $500m in assets
- 10 medium institutions: between $500m to $1b in assets
- 20 large institutions: more than $1b in assets

Q2: How often does your institution review its compliance with the Privacy Act 1988 and the APPs, including with respect to credit reporting and the collection, storage, use and disclosure of personal and financial information?

	Micro	Small	Medium	Large	**Total**	In %
Quarterly	4	1	0	1	**6**	9%
Semi-annually	0	2	0	1	**3**	4%
Annually	16	1	4	10	**31**	46%
Biennially	3	4	1	3	**11**	16%
Other	4	2	5	5	**16**	24%

Q3: When was your last privacy compliance review?

	Micro	Small	Medium	Large	**Total**	In %
Within the last six months	13	8	3	7	**31**	46%
Within the last year	8	1	3	5	**17**	25%
Within the last 18 months	3	1	0	2	**6**	9%
More than two years ago	0	0	3	0	**3**	4%
Other	3	0	1	6	**10**	15%

Q4: How do you make your Privacy Policy available to your customers as per Section D23.5?

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
On website	27	10	10	20	**67**	100%
Sent by mail/email upon request	22	10	10	18	**60**	90%
As part of regular documents sent out to customers (e.g. new member packs)	18	6	7	12	**43**	64%
Verbally	7	3	4	9	**23**	34%
Other	2	3	2	4	**11**	16%

Q5: Does your Privacy Policy contain the information listed below?

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
The kinds of personal information that you can collect and hold	26	10	10	20	**66**	99%
How you collect and hold personal information	27	10	10	20	**67**	100%
The purposes for which you collect, hold, use and disclose personal information	27	10	10	20	**67**	100%

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
How a customer may access personal information about the customer that is held by you, and seek correction of such information	27	10	10	20	**67**	100%
How a customer may complain about a breach, and how you will deal with such a complaint	27	10	10	20	**67**	100%
Other	3	1	1	2	**7**	10%

Q6: How do you control employee access to identify personal or sensitive information?

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
Manually	10	6	4	7	**27**	40%
Banking system access restrictions	21	9	9	20	**59**	88%
We do not have a process	0	0	0	0	**0**	0%
Other	3	0	2	5	**10**	15%

Q7: How does your institution determine that the personal or sensitive information that you collect is reasonably necessary, or directly related to, one or more of your functions or activities?

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
Staff Procedures	23	9	9	19	**60**	90%
Independent monitoring & assurance activity	18	3	6	12	**39**	58%
Review of customer information held	13	5	3	10	**31**	46%
Staff controls	13	6	6	5	**30**	45%
Other	2	1	0	5	**8**	12%

Q8: How do you seek consent from your customers before collecting sensitive information about the customer if the information is reasonably necessary, or directly related to, one or more of your functions or activities?

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
Seek consent verbally	16	7	8	11	**42**	63%
Seek consent in writing	20	7	10	15	**52**	78%
Other	6	2	0	5	**13**	19%

Q9: Describe your process for managing and/or handling unsolicited personal information (e.g. member information received from another member or government agency requests)?

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
Determine if you could or could not have collected the personal information	14	6	3	10	**33**	49%
Determine if the information is necessary	22	5	5	15	**47**	70%
Destroy the information if practicable	18	8	8	16	**50**	75%
De-identify the information if practicable	13	5	3	11	**32**	48%
Other	3	2	2	4	**11**	16%

Q11: How do you advise your customer that you have disclosed private and confidential information to another party as per exemptions listed in Section 23.2?

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
Verbally	6	7	13	8	**34**	51%
In writing	17	6	8	12	**43**	64%
Online	9	2	6	9	**26**	39%
Other	8	2	2	7	**19**	28%

Q12: How may a customer request not to receive direct marketing communications?

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
Verbally	20	10	10	20	**60**	90%
In writing	10	10	22	20	**62**	93%
Opt-out upon receipt of an electronic communication from your institution	21	9	8	19	**57**	85%
Completion of an online form	6	1	3	7	**17**	25%
Completion of a paper form	6	2	4	8	**20**	30%
Other	7	1	0	4	**12**	18%

Q13: In each direct marketing communication with the customer, do you include an opt-out statement or other clause to inform the customer how they can make a request to not receive direct marketing communications?

	Micro	Small	Medium	Large	**Total**	In %
Yes, rely on a general “click here for our privacy policy” in disclaimer	3	0	1	3	**7**	10%
Yes, other	13	10	8	16	**47**	70%
No,	4	0	0	0	**4**	6%
Other	7	0	1	1	**9**	13%

Q14: What reasonable steps does your institution undertake to ensure that information they collect, use or disclose is complete, accurate and up-to-date?

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
Manual review of information by employees before or after collection, use and disclosure	23	8	8	17	**56**	84%
Automated review of information collected	1	2	3	4	**10**	15%
Updating information once notified by the consumer or authorised third party	24	9	10	20	**63**	94%
Updating information provided by unauthorised or unrelated third parties	2	1	1	1	**5**	7%
Regular system or systematic review of data held to verify its adequacy	10	5	3	10	**28**	42%
Other	1	5	2	5	**13**	19%

Q15: How do you define 'promptly' when updating errors brought to your attention by your customer regarding information held by your institution as per Section 23.4?

	Micro	Small	Medium	Large	**Total**	In %
Within 24 hours	18	4	6	9	**37**	55%
Within 48 hours	7	3	0	0	**10**	15%
Within one week	0	1	0	1	**2**	3%
Not defined	1	1	1	6	**9**	13%
Other	1	1	3	4	**9**	13%

Q16: What reasonable steps has your institution undertaken to ensure that information they hold is protected from theft, unauthorised access or disclosure and loss?

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
Document storage security policies	26	9	9	19	**63**	94%
Controlled access to our physical buildings	25	10	10	20	**65**	97%
Verifying the identity of the individual requesting the information	24	10	10	20	**64**	96%
Data security measures	27	10	10	18	**65**	97%
Electronic security systems, such as firewalls, virus software and data encryption on your website	26	10	10	20	**66**	99%
Limiting access to employees on a needs basis	22	9	10	20	**61**	91%
Confidentiality requirements of employees	24	8	10	19	**61**	91%
Staff training	27	10	10	20	**67**	100%
Other	1	0	0	2	**3**	4%

Q17: How often do you review the adequacy of security arrangements of your banking and payment services to protect personal and financial information from misuse, loss or unauthorised access modification or disclosure as per Section 23.3?

	Micro	Small	Medium	Large	**Total**	In %
Quarterly	6	3	1	0	**10**	15%
Semi-annually	2	1	0	1	**4**	6%
Annually	16	5	5	11	**37**	55%
Other	3	1	4	8	**16**	24%

Q18: When was your last review regarding the security and reliability of your data?

	Micro	Small	Medium	Large	**Total**	In %
Within the last six months	17	6	6	13	**42**	63%
Within the last year	10	3	3	5	**21**	31%
Within the last 18 months	0	0	1	0	**1**	1%
Other	0	1	0	2	**3**	4%

Q19: What reasonable steps has your institution undertaken to deal with paper-based information when these are no longer required for any purpose?

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
Returning documents to the customer	6	3	4	4	**17**	25%
Destroying documents in a secure manner	27	10	10	19	**66**	99%
De-identifying the documents	10	2	3	12	**27**	40%
Other	1	0	0	3	**4**	6%

Q20: What reasonable steps has your institution undertaken to deal with digital data information when these are no longer required for any purpose?

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
Returning data to the customer	0	2	0	0	**2**	3%
Destroying data in a secure manner	23	9	8	15	**55**	82%
De-identifying the data	5	3	2	9	**19**	28%
Other	5	1	3	6	**15**	22%

Q21: What is the average timeframe for your response to a customer's request for access to their personal information?

	Micro	Small	Medium	Large	**Total**	In %
Within 5 days	16	7	4	12	**39**	58%
Within 30 days	1	0	3	3	**7**	10%
Timeframe not measured/captured	5	3	1	4	**13**	19%
Other	5	0	2	1	**8**	12%

Q22: If you refuse to provide access to personal information, do you provide the consumer a written notice stating the reasons for the refusal and the mechanisms available to complain?

	Micro	Small	Medium	Large	**Total**	In %
Yes	17	6	8	15	**46**	69%
No	0	0	1	0	**1**	1%
Other	10	4	1	5	**20**	30%

Q23: Do you charge a fee to customers who request access to their personal information?

	Micro	Small	Medium	Large	**Total**	In %
Yes	3	2	3	7	**15**	22%
No	19	6	4	9	**38**	57%
Other	5	2	3	4	**14**	21%

Q24: What information do you provide to a loan guarantor on request?

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
The debtors combined loan, savings and transactional account statements	1	2	2	3	**8**	12%
The debtors loan payment history	17	7	9	14	**47**	70%
The debtors loan balance	18	9	10	16	**53**	79%

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
The debtors loan amounts that are currently overdue and dates they became due	21	8	10	15	**54**	81%
Other	11	1	2	8	**22**	33%

Q25: What reasonable steps does your institution undertake to correct personal information if it is inaccurate, out-of-date, incomplete, irrelevant or misleading?

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
Contacting the relevant customer to update the information	25	10	10	20	**65**	97%
Updating the information with more accurate, up-to-date, complete or relevant information from third parties	7	2	3	10	**22**	33%
Removing the information from your system once detected as being inaccurate, out-of-date, incomplete, irrelevant or misleading	23	7	8	14	**52**	78%
Contacting all relevant third parties whom you have disclosed the inaccurate, out-of-date, incomplete, irrelevant or misleading information to	8	6	3	10	**27**	40%
Other	1	0	0	3	**4**	6%

Q26: Do you train all staff regardless of position in compliance with Section D23?

	Micro	Small	Medium	Large	**Total**	In %
Yes, all staff receive training regardless of position or interaction with customers	26	10	7	19	**62**	93%
No, only customer facing/advice giving staff receive training	1	0	2	0	**3**	4%
Other	0	0	1	1	**2**	3%

Q27: How do you train staff in compliance with Section D23?

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
In-house training	23	9	8	18	**58**	87%
External training	10	4	2	6	**22**	33%
Staff meetings	22	6	6	13	**47**	70%
Staff information sheets	11	4	1	10	**26**	39%
Intranet	6	8	5	14	**33**	49%
Other	5	2	4	3	**14**	21%

Q28: How do you make staff aware of any breaches/complaints that occurred within your institution concerning Section D23?

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
In-house training	20	8	6	13	**47**	70%
External training	2	2	0	3	**7**	10%
Staff meetings	26	6	6	15	**53**	79%

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
Staff information sheets	6	5	1	6	**18**	27%
Intranet	2	5	0	6	**13**	19%
Other	5	2	5	11	**23**	34%

Q29: Please rate the following issues and main causes as the most likely to have occurred in your business.

Multiple selection allowed	never happened	has occurred at least once in the last 36 months	has occurred at least once in the last 24months	has occurred at least once in the last 12 months	has occurred at least once in the last 6 months	has occurred at least once in the last month
Micro institution						
Human processing error (individual releasing the personal information of another person by mistake)	12	8	2	4	1	0
Insufficient training (individual releasing the personal information of another person due to lack of knowledge in privacy obligations)	23	2	2	0	0	0
Third party provider error (such as mail house mistakenly sending details out to the wrong address)	17	6	2	2	0	0
Technical error (system mistakenly providing personal information to the wrong person)	24	1	1	1	0	0
Unauthorised access (employees accessing or disclosing personal information outside the requirements or authorisation of their employment)	23	1	2	0	1	0
Malicious actions (such as data theft or 'hacking')	26	1	0	0	0	0
Other	24	2	0	0	1	0
Small institutions						
Human processing error (individual releasing the personal information of another person by mistake)	1	4	1	1	3	0
Insufficient training (individual releasing the personal information of another person due to lack of knowledge in privacy obligations)	8	1	1	0	0	0
Third party provider error (such as mail house mistakenly sending details out to the wrong address)	5	2	1	2	0	0
Technical error (system mistakenly providing personal information to the wrong person)	10	0	0	0	0	0

Multiple selection allowed	never happened	has occurred at least once in the last 36 months	has occurred at least once in the last 24months	has occurred at least once in the last 12 months	has occurred at least once in the last 6 months	has occurred at least once in the last month
Unauthorised access (employees accessing or disclosing personal information outside the requirements or authorisation of their employment)	10	0	0	0	0	0
Malicious actions (such as data theft or 'hacking')	9	0	1	0	0	0
Other	9	0	0	0	1	0
Medium institutions						
Human processing error (individual releasing the personal information of another person by mistake)	1	1	1	1	5	1
Insufficient training (individual releasing the personal information of another person due to lack of knowledge in privacy obligations)	5	2	0	2	1	0
Third party provider error (such as mail house mistakenly sending details out to the wrong address)	6	1	0	3	0	0
Technical error (system mistakenly providing personal information to the wrong person)	9	0	0	0	1	0
Unauthorised access (employees accessing or disclosing personal information outside the requirements or authorisation of their employment)	6	1	2	0	0	1
Malicious actions (such as data theft or 'hacking')	10	0	0	0	0	0
Other	10	0	0	0	0	0
Large institutions						
Human processing error (individual releasing the personal information of another person by mistake)	2	1	0	2	9	6
Insufficient training (individual releasing the personal information of another person due to lack of knowledge in privacy obligations)	7	4	4	4	1	0
Third party provider error (such as mail house mistakenly sending details out to the wrong address)	3	3	3	6	3	2
Technical error (system mistakenly providing personal information to the wrong person)	9	3	3	3	2	0

Multiple selection allowed	never happened	has occurred at least once in the last 36 months	has occurred at least once in the last 24months	has occurred at least once in the last 12 months	has occurred at least once in the last 6 months	has occurred at least once in the last month
Unauthorised access (employees accessing or disclosing personal information outside the requirements or authorisation of their employment)	12	2	1	4	0	1
Malicious actions (such as data theft or 'hacking')	18	1	0	0	1	0
Other	14	2	1	3	0	0
Total						
Human processing error (individual releasing the personal information of another person by mistake)	16	14	4	8	18	7
Insufficient training (individual releasing the personal information of another person due to lack of knowledge in privacy obligations)	43	9	7	6	2	0
Third party provider error (such as mail house mistakenly sending details out to the wrong address)	31	12	6	10	6	2
Technical error (system mistakenly providing personal information to the wrong person)	52	4	4	4	3	0
Unauthorised access (employees accessing or disclosing personal information outside the requirements or authorisation of their employment)	51	4	5	4	1	2
Malicious actions (such as data theft or 'hacking')	63	2	1	0	1	0
Other	57	4	1	3	2	0

Q30: What percentage of breaches or incidents relating to Privacy are systemic in nature? (Please comment)

	Micro	Small	Medium	Large	**Total**	In %
Nil	23	7	7	15	**52**	78%
Less than 1%	1	3	1	4	**9**	13%
1%	1	0	0	0	**1**	1%
5%	1	0	0	0	**1**	1%
10%	0	0	1	0	**1**	1%
20%	1	0	0	0	**1**	1%
30%	0	0	1	0	**1**	1%
50%	0	0	0	0	**1**	1%

Q31: Please advise how often remedial action has been required in response to a Privacy breach or complaint within your institution, and what that remediation activity has included. (Please advise numbers and commentary if necessary)

Multiple selection allowed	Micro	Small	Medium	Large	**Total**	In %
Minor – Customer request/access granted / data corrected / Staff Feedback	5	5	5	10	**25**	37%
Moderate – Apology / Acknowledgement of error/ Staff Training / Procedure Change	13	5	7	13	**38**	57%
Significant – Multiple or Systemic Customer Remediation / Report to Regulator / Business Continuity Crisis Management	0	0	0	1	**1**	1%
Other	11	1	1	5	**18**	27%